WINTER/SPRING 2002 VOL. 2

The Center Link

CENTER FOR INFORMATION TECHNOLOGY

Where CIT Connects

in this issue

IT SECURITY— what you can do

CIT's Newest Citizen

CIT 2001 Annual Awards Ceremony

What does the American flag mean to you? Were you born under it or did you have to earn it? Did you fly it, wear it, salute it, treasure it before September 11th? How many naturalized citizens do you know? One more question:

How many smiles can fit in a moment on a perfect July day?

Answer...

at least this many...

Jinyuan Duan takes it "phonetically" easy on his many friends and colleagues. At the Center for Information Technology (CIT) he goes by J.D. That's him - fourth from the left - first row. That beaming person to his right is Lisa Woodward. (In July 2001 they were very serious about each other. In November 2001 they married.) The rest of the gang should look familiar - if just a little out of their ordinary CIT context.

How did J.D. get to this perfect July day? To become a naturalized U.S. citizen one must maintain five-years of permanent residency, demonstrate a good moral character, pass a civics exam, swear an oath of allegiance, and you're in. Oh yes, and please make sure your tax obligations are paid in full! J.D. came to America in 1987 to successfully pursue his Masters Degree in Computational Linguistics at Georgetown University. His close-knit and loving family supported his decision. The youngest of three sons, J.D. was born in Yuncheng, a good-size town of about 50,000 persons, in the Shanxi Province of the People's Republic of China.

continued on page 3

From the Director

Al Graeff

Dear CIT Colleagues,

As I prepared my notes for this column, it was natural to look back at the year 2001. At our December 12, 2001 CIT Annual Awards Ceremony I spoke of our commitment to a greater good and our role within NIH and the Department of Health and Human Services (DHHS). As I said at our awards ceremony, *"It's a credit to CIT that you've earned the respect of the Department and the respect of the NIH".* Over the last year, we have successfully met many challenges. In the year before us, I know that we can count on each other to meet those that lie ahead.

In our inaugural issue of **The Center Link, *Where CIT Connects***, I promised that our publication would celebrate the people who come to work here each day and do their part, and more, to make the CIT vision happen. I'm happy to report that for me, this column is shaping up to be one of my easier jobs. The breadth and depth of our talent is exceptional.

In this Winter 2002 issue we highlight IT security, a topic that is both timely and central to our success as the principal provider of IT services to NIH. You'll find a story on the NIH Incident Response Team (IRT) and their recent Guardian Award from the Office of Personnel Management (OPM). While this piece focuses on the mission of the IRT, successful IT security truly cuts across every division and every desktop at CIT and the NIH. From mainframe to desktop, we can be proud of the complexity and diversity of CIT contributions to this vital area.

Lastly, I invite you to read an inspirational "After-the-Log-off" article and a profile of one of our colleagues. The year 2001 is forever marked, and as we move forward into the challenges and opportunities of year 2002, it's good to know the caliber and constancy of our CIT colleagues. It's important to know that we can count on each other.

Enjoy.

IT Security IT'S ALL ABOUT PEOPLE

Individuals, businesses of all sizes, and local, state and federal government agencies have a common information technology (IT) need ...to protect their private or confidential data, communications, and computing environment. We know that intrusion attempts on federal systems are increasing in number and complexity. Cyberterrorism is a potent threat. Across the NIH, at-risk data may include patient records, personnel and payroll records, and biomedical research findings. To secure their systems, most individual, corporate, and government users employ a range of advanced technologies, including intrusion detection software, firewalls, vulnerability scans, and anti-virus software.

Standing from left to right:

Rick Hargett
NIH Senior Information Systems Security Officer, (IRT Coordinator)
CIT, Office of the Deputy Chief Information Officer (ODCIO)

Kevin Brownstein
CIT, Division of Network Systems & Telecommunications (DNST)
Network & Engineering Branch/Network Security Section

Khiem Tran,Computer Engineer, CIT, DNST, Network and Engineering Branch, Network Security Section

Brian Hoang, Network Security Section Chief (acting) CIT, DNST, Network & Engineering Branch/Network Security Section

Julia Lin
CIT, DNST, Network & Engineering Branch/Network Security Section

Jaren Doherty
Information Security and Awareness Office Director
CIT, ODCIO, NIH

Robert Todd, Security Consultant, Advanced Research Corporation

Scott W. Sloan, Network Security Engineer, CIT, DNST, Network & Engineering Branch/Network Security Section

Dawn Farr, CISSP, CIT Information Systems Security Officer, CIT, ODCIO, NIH

Lee Sommer, Director of Information Systems, CETECH, Inc.

Seated from left to right:

Dr. Ruth Kirschstein, Acting Director, National Institutes of Health

Alan S. Graeff, CIO NIH/Director, CIT

Dona Lenkin, Deputy CIO, NIH, Deputy Director, ODCIO

continued on page four

THE PLEDGE OF ALLEGIANCE

"I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one Nation under God, indivisible, with liberty and justice for all."

continued from cover

J.D. is the only son who lives outside of China. He is devoted to his family and has returned to visit them many times. We learned from his friend that J.D. once flew to China to escort his now elderly mother to his American home. After a successful visit, he escorted her home to China, to guarantee her comfort and safety.

According to J.D.'s best friend (and best man) Patrick Booher,

"J.D. seems to set a goal and then just keeps on going until he achieves it ...for example, when he began to take MicroSoft certification courses, he literally pulled the plug on his TV and put it in a closet until he had completed all the individual certification components.

...J.D. is one of those refreshing people you meet and like instantly. You know you can trust him to be there for you whatever comes".

J.D. loves his work as a Systems Administrator with BOSB (that's the Back Office Systems Branch) at CIT. He's glad his academic path led him to CIT some three years ago. J.D. notes that since his arrival, his boss (Kevin Hobson) has helped him expand his vocabulary in ways he never would have expected.

J.D.'s CIT colleagues are glad he's part of their team. When they organized a unique celebration for his Oath Day, J.D. was overwhelmed by their friendship and support. We asked, "did you know that your CIT friends were coming?" J.D. said,

"Yes, it was thrilling. I was so touched. But I didn't know that I was the only person with a group like that, the balloons, the banners ...and I had a big surprise the following week ... my cubicle was patriotically decorated and there was a giant greeting card with lots of CIT signatures on it!"

My CIT friends are like my family. At our wedding, they were my family. My Chinese family could not come. Our wedding was small and they came and stood for me.

And about that oath of allegiance, we asked J.D., "What was it like to take the oath? What did you think?" and he said,

"It was profound. I didn't choke, but all I could think was that life had changed - new responsibilities - new learnings. I felt so fortunate, so grateful for the new life, and to have Lisa in it."

In closing, we have one more question for the reader.

Did you know that in Mandarin Chinese "America" literally translates to "Beautiful Country"? Jinyuan Duan clued us in. When asked, "what does the flag mean to you?" J.D. quietly and clearly answered,

"a brand new life, a new hope, a new attitude".

And on that note...

Congratulations J.D.!

IT Security

continued from page 2

But merely applying sophisticated technology does not guarantee a successful IT security program. Successful IT security is all about people - from the dedicated professionals who design, maintain, and implement IT security to the end users - those who pay attention to and follow basic security guidelines. At the NIH, the frontline for IT security is found at the Center for Information Technology (CIT), home of the NIH Incident Response Team (IRT). Led by CIT's Office of the Deputy CIO, NIH, the IRT represents the very best in innovative and vigilant IT security.

Since its inception in July of 1998, the IRT has helped ensure the security of diverse NIH systems, data, and biomedical research information while maintaining connectivity and interoperability throughout NIH. The IRT serves as the focal point for information security incidents across NIH by:

- identifying computer security incidents,
- characterizing the nature and severity of incidents, and
- providing immediate diagnostic and corrective actions when appropriate.

The exceptional contributions of the IRT in ensuring the confidentiality, availability, and integrity of NIH information resources have made the NIH a federal government leader in protecting critical information from unauthorized use. In 2001 the IRT was recognized at the national level for their accomplishments. They won the prestigious Office of Personnel Management (OPM) Guardian Award.

The OPM Guardian Award recognizes agencies, components, or programs that lead the way in finding cost-effective and/or innovative solutions to today's security needs. Previous winners were drawn exclusively from the federal intelligence and defense communities. The IRT can be proud that their success has made the NIH and the Department of Health and Human Services (DHHS) the first civilian agency to achieve this distinction.

As part of its procedure, the IRT conducts automated security audits of all NIH systems to:

- determine vulnerabilities,
- recommend corrective actions, and
- direct resources to the areas most in need of improved security.

The IRT uses trend analysis to determine if effective safeguards are in place. The IRT tracks and closes out incidents through a secure, automated system and distributes weekly status reports to key DHHS personnel. IRT reports identify, categorize, and prioritize vulnerabilities and then recommend corrective actions. In 2001 the IRT successfully remediated all confirmed compromises of NIH systems.

The IRT helps users protect systems by blocking sites that are attacking other organizations, and warns other agencies about upcoming attacks by exchanging information with Federal incident response organizations. The NIH Letter of Agreement with the Federal Computer Incident Response Capability (FedCIRC) Program provides a mechanism for the IRT and FedCIRC to work together to:

- handle security incidents,
- share related information,
- solve common security problems, and
- plan future infrastructure protection strategies.

This mutual exchange of information aids in damage containment and recovery from computer or network related security incidents.

The IRT also coordinates incident prevention and response with the:

- Forum of Incident Response and Security Teams (FIRST),
- Department of Energy's Computer Incident Advisory Capability (CIAC),
- Federal Computer Security Managers Forum, and other organizations.

What is the secret of their success ?

IT'S ALL ABOUT COMMUNICATION

The IRT has established open and trusted communication channels across the NIH. IRT experts are available to assist NIH system administrators 24 hours a day, seven days a week, from investigating incidents to repairing compromised systems. The IRT continuously monitors all incoming internet traffic to detect and prevent specific cyber security exploits. When the IRT detects real or probable malicious activity, quick steps are applied to prevent unauthorized access to NIH systems and networks. The goal is to minimize the impact of such activity. The IRT then distributes Security Advisories to 28 NIH Institutes and Centers (ICs). Each IRT Security Advisory warns of exploits and recommends actions. IRT Security Advisories, guidelines, and procedures are available on the IT security pages of the CIT website, http://cit.nih.gov/security.html. All guidelines and procedures are developed based on best practices, in close collaboration with NIH Institute and Center technical personnel, Information System Security Officers (ISSO's) and the IRT.

What's Next?

The IRT is currently piloting a secure tracking vehicle with several NIH Institutes and Centers. The tracking vehicle will be used to identify each vulnerability and the status of remediation down to the individual desktop machine. This system will enable the IRT to:

- test and validate which vulnerabilities have been repaired,
- which ones are false positives, and
- which ones are still in need of corrective action.

In addition, the IRT works with the FBI, Secret Service, and other international law enforcement agencies in investigating attempts to break into NIH systems or when there is a coordinated attack against multiple organizations.

In their spare time, IRT personnel:

- conduct periodic security training courses as part of CIT's free training program,
- provide presentations to Information System Security Officers (ISSOs) and other management and technical personnel,
- achieve Certified Information Systems Security Professional (CISSP) certifications, and
- participate in SANS network security training courses.

How Can You Help?

IT security is central to CIT's success as the principal provider of IT services to NIH. So what can we as individuals do to help? We can pay attention. Why not choose security.nih.gov as a preference on your portal page? Take a few moments to see what's new.

We can mark our calendars for on-line IT security training every twelve months http://irm.cit.nih.gov/sectrain/ and then do it.

We can take practical steps to secure wireless devices, use the "lock workstation" feature on our desktops to secure them every time we step away, and shut down and log-off our systems every night. According to the IRT, every action makes a difference.

As their nomination for the 2001 OPM Guardian Award so clearly states,

"They have exhibited excellent management and technical expertise in preventing and responding to potentially serious security problems that could jeopardize the ability of NIH to carry out its mission. By continuously improving the IT security of NIH while adapting to a rapidly changing technology environment, the IRT also provides leadership to incident response capabilities of DHHS Operating Divisions and serves as a model for incident response groups of other Federal Government agencies."

continued on page six

Here's A Good Example of Why People Make the Difference!

From: ##### (CIT)

To: CIT DCS HD Staff

Subject: IMPORTANT, PLEASE READ: FW: Kudos to TASC FW: Password Help

Everyone… Please read below about the incident that happened yesterday … to be aware and alert of this potentially happening again… Both ### (the customer's ISSO) and the IRT got involved quickly and it has been referred on to the Inspector General's office.

If you get any calls or e-mails from someone reporting that e-mail(s) are being sent under their name but they didn't send them, please contact someone in the TASC Antivirus/Security group asap and we will notify the IRT. Thanks for your attention to this important matter.

From: #### (IRT)

To: #### (CIT) #### (CIT)

Subject: Kudos to TASC FW: Password Help

and ####, I wanted to bring this to your attention. TASC did a great job. A user sent an e-mail requesting their user ID and password for ITAS. They left a phone number in their message. When TASC went to call them, they realized it was a different phone number than that in the global listing. As it turns out, the user had no knowledge of the e-mail and had never made the request.

I've been working with the ISSO on this one, and the case has now been referred to the IG. As I mentioned to #### below, you may want to give other TASC members a heads up, as we don't know what this person's intent was.

IT Security

continued

If you ask the members of the IRT, they'll be the first to tell you that successful IT security truly cuts across every division and every desktop at CIT and the NIH.They are quick to compliment their colleagues at CIT and across the NIH. The IRT recognizes that technology is only as effective as the people who use it. IT security procedures are only as effective as the people who read, understand, and follow them. IRT assistance is available through CIT's Technical Assistance Support Center (TASC) at 301-594-6248. If you have questions about the IRT, please contact Dawn Farr, CIT Information System Security Officer, at 301-402-4449 or send her an e-mail dfarr@mail.nih.gov.

USEFUL WEBSITES AND CONTACT INFORMATION:

Your central source for cyber and physical security information at NIH:

http://security.nih.gov

NIH Information System Security Officers:

http://irm.cit.nih.gov/nihsecurity/scroster.html

TASC Customer Support:

http://support.cit.nih.gov/

Phone: 301-594-6248 (GoCIT)

Antivirus updates for technical users:

http://www.antivirus.nih.gov/

Security alert information for general users:

http://securitynews.nih.gov/

Security incident reporting guidelines:

http://irm.cit.nih.gov/security/ir_guidelines.html

FAQs about NIH's IT Security Program:

http://irm.cit.nih.gov/nihsecurity/secfaqnih.htm

DESKTOP TO DESKTOP

From the ODCIO

WHAT YOU CAN DO

To report a computer security incident, contact your IC help desk, ISSO, or TASC (301-594-6248) (GoCIT).

Be wary of suspicious, unsolicited e-mail attachments.

Assume responsibility for your own computer security.

Secure your desktop every time you step away by using the lock workstation feature.

Shut down and log-off every night.

Choose a strong password-Make it:

- random and change it often!
- memorable--don't write it down!
- secure - don't share it or post it near your desk!
- hard to crack - use a mix of upper and lower case, alpha and numeric characters!

Backup important files on a daily basis.

Know general security information and policies http://www.cit.nih.gov/security.html.

Beware installing screen savers or games from unknown sources.

Make sure system security patches are installed periodically on both your desktop and any laptops. Check with your system administrator if you have questions.

Keep antiviral software up-to-date and configured properly on office and home desktops, and any laptops.

Get IT Security training every 12 months http://irm.cit.nih.gov/sectrain/.

EXCERPT: LAB/BRANCH/SECTION CHIEFS MEETING NOTES: AUGUST 2001

Al thanked again all of the hardworking folks at CIT who made "Code Red Worm" another "CIT non-event". Al summarized Code Red Worm as an attack on the net, taking advantage of a hole in Windows NT and Windows 2000. Al observed that this is not the first, nor will it be the last attack, and he particularly saluted the hard work of the DNST staff (at the subnet) and the Incident Response Team (IRT) for their successful management of this threat. Al observed that NIH IT security is managed by boundaries and level of criticality, citing both eRA and the Clinical Center as examples where this approach has been proven successful.

CIT Staff Profile

Charles Mokotoff

Division of Enterprise & Custom Applications

How did you get to CIT?

First arrived as a contractor to DCRT ('94) after stint with the Peace Corps

CIT Webmaster Charles Mokotoff tried to politely say ***"no thanks"***. When we initially asked Charles to be included in our ***Center Link*** staff profiles, Section 508 compliance issues and the unveiling of the NIH Portal project were first on his priority list. When we eventually grabbed a few minutes, it quickly became clear that Charles prefers to focus on his collaborative work, particularly with his CIT colleagues Richard Barnes, Sandy Desautels, and Dale Graham. In his own words,

"They are terrific
... we work well together
... deadlines are tight, but creativity and collegiality really flow."

Richard Barnes, Charles Mokotoff, Dale Graham, Sandy Desautels

Charles summarized his role at CIT as taking the lead for internal and external webspace, making sure that pages are accessible, links are working and any issues are resolved in a timely manner. In the past year, his major focus has been the NIH Portal (http://my.nih.gov). Charles serves as the technical lead for this project, which ties together many of the disparate information systems at the NIH into one web interface. The NIH Portal replaces the CIT Intranet. As Charles explained, he and his team have attempted to "scrape most of the functionality from the existing intranet site and represent it in portal 'modules' - small snippets of web pages that you can place wherever you want". The final product is a site that each user can customize to his or her own professional needs.

Charles also serves as the lead for the NIH Information Technology Management Committee (ITMC) subcommittee dealing with Section 508 web accessibility issues. Section 508 holds particular resonance for Charles. Hearing impaired himself, Charles has long been an advocate for greater usability and accessibility on the web, particularly for the deaf and hearing-impaired community at the NIH. Charles encourages all CITers to check out the site addressing Section 508 (http://508.nih.gov/). And while you're checking out sites, please drop by http://security.nih.gov -- another collaborative success story. Operating on a tight schedule, Charles and his colleagues worked with the NIH Office of Research Support (ORS) to design and produce this one-stop resource for security information at NIH.

So, whether you need information, clarification, or inspiration, Charles invites you to call upon him and his CIT co-workers. If you'd like to discuss classical guitar, Elizabethan lute music or his long-ago debut in the Carnegie Recital Hall, Charles is up for that as well, but that's another story!

Favorite song?
Any Elizabethan lute music

Favorite tree, plant, or flower?
White birch tree

Favorite Book?
Joys & Sorrows, by Pablo Casals

A Few Moments from the...

CIT Annual Awards Ceremony and Director's Report (December 12, 2001)

CIT Director and CIO Al Graeff reviewed some of CIT's accomplishments over the past year, and offered a glimpse of the challenges facing CIT in the coming year. Al noted,

"each of these awards ... is an acknowledgement of all of you and the level of excellence you provide. While (the awards) represent some of the shining efforts of some individuals they are all earned after a shared effort has been made."

Upstairs in Natcher's sun-filled atrium the crowd congratulated the awardees, talked and laughed with their colleagues, and enjoyed light refreshments.

CIT thanks the following volunteers for their assistance with the 2001 CIT Annual Awards Ceremony and Directors' Report:

Justin Bentley, OPEC
Susan Chaffee, OPEC
Bonnie Douglas, OPEC
Wendy Evans, HRMO
Michele France, OPEC
Helen Kling, HRMO
Marie Lagana, OPEC
Mitch Levine, OD
Laurie McClintock, HRMO
Lanny Newman, OPEC
Paula Ptacek, OPEC
Gloria Richardson, OD

The Center Link is produced as an internal publication for CIT employees by the CIT Office of Planning, Evaluation and Communications (OPEC).

OPEC welcomes all editorial comments and suggestions. If you have a news item, article idea, calendar event or photograph you'd like to share, please contact the The Center Link editorial team:

Editor: Michele Mulholland France
Communications Director: Lanny Newman
OPEC Contributors: Marie Lagana, Director, Justin Bentley, Susan Chaffee, Bonnie Douglas, Paula Ptacek, Kevin Sullivan.

CIT The Center Link Editorial Board:
OPEC Contributors
Trish Flock
Kevin Murphy
Chris Ohlandt
Gloria Richardson

CIT
Center for Information Technology

National Institutes of Health
OPEC: Building 12A, Room 4063
Bethesda, MD 20892-5651

Main: 301.496.6203
Fax: 301.402.4437

Web: http://opec.cit.nih.gov
E-mail: centerlink@mail.nih.gov

CIT's Office of Diversity and Employee Concerns (ODEC) is available to answer any diversity or employee question or concern you may have. ODEC expands the functions from the office we knew as "EEO". If you have a question or concern, please do not hesitate to contact CIT's ODEC Officer, Gloria Richardson, at 301.402.2268.